IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA, ex rel. SARAH BEHNKE,	:	**CIVIL ACTION NO. 2:14-cv-00824 (MSG)**
Plaintiffs,	:	
v.	:	
CVS CAREMARK CORPORATION, CVS CAREMARK Rx, LLC (f/k/a CAREMARK Rx, INC.), CAREMARKPCS HEALTH LLC, and SILVERSCRIPT INSURANCE COMPANY,	:	
Defendants.	:	

ORDER
REGARDING THE SEARCH FOR AND PRODUCTION OF DISCOVERY MATERIAL (ESI PROTOCOL)

This Order sets forth the protocol for the production of discovery material in the above captioned litigation, pursuant to the provisions of Rules 26 and 34 of the Federal Rules of Civil Procedure.

1. SCOPE

1.1 Except as specifically limited herein, the procedures and protocols set forth in this ESI Protocol shall govern the search, disclosure, and format of electronically-stored discovery material produced for use in this litigation. This Protocol also contains provisions governing electronic production of hard copy documents.

1.2 This Order is intended to streamline e-discovery to best carry out the requirements set forth in the local rules and the Federal Rules of Civil Procedure, to maximize efficient and quick access to documents, and to minimize related discovery costs, to the extent feasible and appropriate.

1.3 The parties shall meet and confer to try to resolve any disputes that may arise under this ESI Protocol prior to seeking assistance from the Court. Any requesting or producing party may seek to deviate from this ESI Protocol, provided, however, that no requesting or producing party may seek relief from the Court concerning compliance with the ESI Protocol without first describing the deviation in writing and then engaging in good faith meet and confer discussion on the proposed deviation.

1.4 The parties agree that reasonable measures will be taken to preserve potentially discoverable data from alteration or destruction in the ordinary course of business or otherwise.

1.5 To the extent additional obligations or rights not addressed in this Protocol arise under the Federal Rules of Civil Procedure or other applicable law or rules, that law or rule shall govern.

1.6 To the extent there is any conflict between the provisions of this Protocol and the Stipulation for Confidentiality Agreement and Protective Order entered May 13, 2018 (ECF No. 74), or any amended version thereof that may be entered in this matter in the future (collectively, "Protective Order"), the provisions of the Protective Order shall control.

1.7 To the extent possible and appropriate, these protocols shall govern non-party productions.

1.8 This ESI protocol does not address or resolve any objection to the scope of the Parties' respective discovery requests. Nothing in this Protocol shall be deemed to

waive or limit any party's right to object to production, discoverability, admissibility, or confidentiality of data or any other discoverable materials

1.9 Prior productions by any entities are excluded from this Order.

2. DEFINITIONS

2.1 "Document" is defined to be synonymous in meaning and equal in scope to the usage of the term in the Federal Rules of Civil Procedure. For avoidance of doubt, the term "document" shall include hard copy documents and ESI (electronically stored information).

2.2 "Hard copy document" means a document that was maintained in paper or other tangible form.

2.3 "Document family" means, for example, an email and associated attachments, or a document containing embedded files.

2.4 "Backup systems" refers to computer systems used to store copies of information to permit recovery of the information in the event of loss or damage to the original data.

2.5 "Custodian" shall mean any individual of a producing party, as identified and agreed by the parties, as likely having possession, custody, or control of potentially relevant documents.

2.6 "Custodial data source" means any data source used for business purposes in or on which custodian is likely to store potentially relevant documents including, but not limited to, personal computers, laptops, tablets, email (whether stored locally or centrally), mobile devices, shared network servers, shared or individual network folders, cloud storage systems, structured data systems, or social media.

2.7 "Non-custodial data source" means any data source that is not kept or maintained by any particular custodian but which is likely to contain relevant documents, including data sources used by any department, business unit, or division of a producing party, and shared storage systems that may contain relevant documents.

2.8 "Metadata" means: (i) information embedded in or associated with a file that is not ordinarily viewable or printable from the application that generated, edited, or modified such native file which describes the characteristics, origins, custody, usage, and/or validity of the electronic file; and/or (ii) information generated automatically by the operation of a computer or other information technology system when a native file is created, modified, transmitted, deleted, or otherwise manipulated by a user of such system.

2.9 "Search term" means a word or a combination of words or phrases designed to capture potentially responsive documents and includes strings of words or phrases joined by proximity and Boolean connectors or other syntax.

2.10 "TAR" (technology-assisted review) means a machine learning process for prioritizing or coding a collection of documents.

2.11 "Structured data" means data that resides in a fixed field within a record or file, or stored in a structured format, such as databases (such as SAP, JD Edwards, Microsoft Dynamics, Oracle, SQL, Microsoft Access) or data sets, according to specific form and content rules as defined by each field of the database.

2.12 "Unstructured data" refers to free-form data which either does not have a data structure or has a data structure not easily readable by a computer without the use of a specific program designed to interpret the data, including but not limited to,

word processing documents, slide presentations, email, PDFs, spreadsheets, and webpages, blogs, image files, instant messages, audio and video files, and others of similar variable format.

3. PRODUCTION FORMAT. Each producing party shall, to the extent reasonably and technically possible, produce documents according to the specifications provided in Exhibit A: Specifications for the Production of Unstructured Data, as well as the below parameters, except that the production format for each source of structured data will be discussed and agreed to separately by the parties.

3.1 De-Duplication: A producing party may elect to de-duplicate. If a producing party elects to de-duplicate, the producing party shall identify duplicates by the MD5 hash algorithm (or a reasonably equivalent alternative) to create and compare hash values for exact duplicates only. Other methodologies that are substantially different for identification of duplicates must be discussed with the requesting party and approved in writing before implementation. The resulting hash value for each item shall be reflected in the MD5 Hash Value field specified in Exhibit A.

a) Vertical deduplication. A producing party may de-duplicate documents vertically by Custodian, provided however, that an email that includes content in the BCC or other blind copy field shall not be treated as a duplicate of an email that does not include content in the BCC or other blind copy field, even if all remaining content in the email is identical.

b) Horizontal deduplication. A producing party may de-duplicate documents horizontally (globally) across the population of records, if the producing party discloses to the receiving party that it has deduplicated horizontally,

and provided further that: (a) an email that includes content in the BCC or other blind copy field shall not be treated as a duplicate of an email that does not include content in the BCC or other blind copy field, even if all remaining content in the email is identical; and (b) all Custodians who were in possession of a de-duplicated document and the directory structure where the Custodian stored the de-duplicated document must be identified in the "Custodian – All" Metadata field specified in Exhibit A.

3.2 E-mail Thread Suppression: Email threads are email communications that contain prior or lesser-included email communications. A most inclusive email thread is one that contains all of the prior or lesser-included emails and attachments, including each branch of the email thread. To the extent a producing party intends to suppress lesser-included emails, they shall meet and confer with the requesting party regarding whether it is appropriate and the appropriate means to do so.

3.3 Unitization: In scanning hard copy documents, producing parties shall take reasonable steps to avoid distinct documents from being merged into a single record, and single documents from being split into multiple records. The producing party shall take reasonable steps to physically unitize hard copy documents. Documents stored in a binder, folder, or similar container (each, a "container") shall be produced in the same order as they appear in the container. Similarly, pages that are stapled or clipped shall be produced as a single document and not multiple one-page documents.

3.4 Redacted Documents: In the event a document is redacted, the full text should be replaced with OCR text that excludes the redacted material.

a) When a TIFF image is redacted, the TIFF image should show the word "redacted" where applicable and a production Load File field should be populated to indicate the document contains a redaction.

b) If a document to be produced in native format requires redaction then it should be produced in redacted native format. The native file should show the word "redacted" where applicable and a production Load File field should be populated to indicate the native file contains a redaction.

3.5 Text Files. Each document produced under this ESI Protocol shall be accompanied by a single, multipage text file containing all of the text for that document (as opposed to one text file per page of such document). Each text file shall be named using the Bates number of the first page of the corresponding production item. The text of each file shall be extracted directly from the native file. There is no obligation to OCR any electronic documents that do not natively exist in a text-searchable form, but to the extent feasible, a producing party will apply OCR software to such a document so that the full resulting text shall be provided on a document-level basis in an appropriately formatted text file (.txt) that is named to match the first Bates number of the document. Text files shall be provided in a "text" folder. To the extent that a document is redacted, the text files shall not contain the text of the redacted portions but shall indicate where the redactions were made (e.g. with the notation "redacted").

3.6 Attachments: Email attachments and embedded files must be mapped to their parent document by the Bates number by including a "Beg Attach" field designating the beginning of each such attachment and "End Attach" field

designating the end of each such attachment. If attachments and embedded files cannot be separated from their parent documents, then "Beg Attach" and "End Attach" fields listing the unique beginning and end number for each attachment or embedded document must be included. Non-substantive automatically-generated embedded files, such as logos, embedded, non-substantive formatting files such as .ole or .dll formats, or confidentiality legends need not be produced as separate attachments. To the extent they are maintained together, all documents in a document family shall be consecutively Bates number stamped with the child documents produced immediately after the parent document.

3.7 Password Protected Files: The producing party shall make reasonable efforts to ensure that all encrypted or password-protected documents are successfully processed for review and production under the requirements of this ESI Protocol, and the decrypted document is produced. To the extent such documents are not successfully processed, the producing party agrees to: (a) produce a slipsheet for each encrypted or password protected document that cannot be successfully processed indicating that the document cannot be decrypted; and (b) provide the metadata for the document required by Exhibit A to the extent it can be reasonably extracted from the file in its encrypted form.

3.8 Embedded Documents: Embedded documents (e.g. a spread sheet embedded within a word processing document) will be extracted, produced as an independent document, and related back to the respective top-level parent document (e.g., standalone file, email message, tec.) via the "Beg Attach" and

"End Attach" fields referenced in Exhibit A. Related embedded documents will be produced within a continuous Bates range

3.9 Compressed and Container Files: Compression file types (e.g., .CAB, .GZ, .RAR. .ZIP), shall be decompressed to ensure that a compressed file within a compressed file are decompressed into the lowest possible compression resulting in individual folders and/or files. Original compression files and container files need not be produced, provided the responsive content files are produced in accordance with the specifications of this ESI Protocol.

4. STRUCTURED DATA FORMAT

4.1 The parties will meet and confer to discuss a data extraction for specific information contained in particular databases. Provision of a sample extraction may be useful for these discussions. After meet and confer consultation, the producing party may opt to produce relevant and responsive information from databases by querying the database for discoverable information and generating a report in a reasonably usable and exportable electronic format (*e.g.*, in Microsoft Excel™ or .csv format).

5. IDENTIFICATION PROCESS REGARDING CUSTODIANS AND SOURCES OF DOCUMENTS

5.1 Process for Determination of Custodians: The parties shall meet and confer as necessary regarding appropriate custodians. Prior to a scheduled meet and confer between the parties to discuss appropriate custodians, the producing party shall identify proposed custodians by name, job title(s), and years of employment.

5.2 Process for Determination of Custodial and Non-Custodial Data Sources: The parties shall meet and confer as necessary concerning appropriate custodial data

sources and non-custodial data sources. Prior to a scheduled meet and confer between the parties to discuss appropriate custodial data sources and non-custodial data sources, the producing party shall identify custodial data sources and non-custodial data sources. For each custodial data source or non-custodial source(s) identified that a producing party contends is not reasonably accessible, the producing party shall identify why the information is considered not reasonably accessible and the general nature of such software, systems, or information.

6. SEARCH METHODOLOGY FOR UNSTRUCTURED DATA

6.1 Search Methodology Disclosures. The parties hereby agree that negotiations regarding search terms and other filtering methods are intended to be a cooperative and iterative process, involving a good faith exchange of information and proposals to facilitate the negotiations. Prior to conducting a search for responsive documents, regardless of the search methodologies to be employed, the parties shall meet and confer regarding the search methodologies the producing party proposes to employ to identify potentially responsive documents, and make such disclosures regarding their proposed search methodology that will permit the requesting party to evaluate the proposed methodology and enable meaningful meet and confers. Such disclosures should include whether the producing party intends to fulfill its obligation to produce responsive documents by either: (i) producing all non-privileged documents that meet specified, agreed-to search term or other filtering criteria, or (ii) subjecting documents that meet specified, disclosed search terms or other filtering criteria to any human or automated responsiveness review.

6.2 Search Term Development Process. To the extent a producing party elects to use search terms, the producing party shall propose an initial list of the search terms that the producing party intends to use, after which the parties shall promptly meet and confer to attempt to reach agreement on the search terms. To the extent that a requesting party proposes additional or modified search terms that a producing party asserts are unreasonably overbroad or otherwise objectionable, the parties will meet and confer to discuss in good faith regarding any disputed terms. The producing party will, upon reasonable request, provide hit reports and other metrics to facilitate these discussions.

6.3 Process for Other Proposed Filtering Methods. If a producing party discloses that it intends to use other filtering methods besides applying search terms (e.g., TAR or similar advanced analytics and time periods) as a means of including or excluding documents to be reviewed for responsiveness or of culling or otherwise limiting the volume of information to be reviewed for responsiveness, prior to use of such tool the parties shall meet and confer regarding the appropriateness of the proposed filtering method and how it is to be applied.

7. ASSERTIONS OF PRIVILEGE & REDACTION

7.1 Pursuant to Rule 26(b)(5) of the Federal Rules of Civil Procedure, the parties hereby agree that a producing party may redact or, to the extent necessary, withhold a document if it is protected by attorney-client privilege, the work-product doctrine, or other reasonably applicable privilege from disclosure, or as required by law.

7.2 The following are acceptable formats for privilege logs:

a) Privilege logs shall be provided in Excel format and shall contain, to the extent such information is reasonably available, the following information for each responsive document withheld or redacted: (i) a sequential number associated with each privilege log record; (ii) the date of the document; (iii) the Bates numbers (if a document has been produced in redacted form); (iv) the identity of person(s) who authored or sent the document, including identification of which of them are attorneys; (v) the identity of person(s) who received the document, including identification of which of them are attorneys; (v) a general description of the subject matter of the information contained in the document that, without revealing information itself privileged or protected, is sufficient to understand the subject matter of the document and the basis of the claim of privilege or immunity; (vi) the type or nature of the privilege asserted; and (vii) an indication of whether the document has been redacted and produced or withheld in its entirety. If a producing party identifies portions of a document and redacts such portions of the document pursuant to this ESI Protocol the producing party must log the fact of each document's redaction.

b) As an alternative to manually entering the information required in the section above, specifically subsections (a)(i)-(v), a portion of each producing party's privilege log may be generated by exporting objective metadata from the review tool used to identify privileged or work-product protected documents where the objective metadata provides the information required under the section above. Such metadata shall include

the following: (i) A unique privilege log identifier or, in the case of redacted documents, the Bates number assigned to such document; (2) Author/Custodian; (3) From; (4) To; (5) CC; (6) BCC; (7) date sent, received, or created; (8) document type (e.g., message, attachment, loose file); (9) file name, (10) file size, and (11) page count.

7.3 Should a receiving party be unable to ascertain whether or not a document contained on the log is privileged or have reason to believe a particular entry on the log is responsive and does not reflect privileged information, the parties shall meet and confer to attempt to cooperatively resolve the dispute.

7.4 To the extent a producing party redacts documents other than for reasonably applicable privilege or as required by law, the producing party shall notify the receiving party of the reason(s) for doing so and provide a redaction log which shall (1) identify each such document by bates numbers, and (2) provide for each such document a description of the basis of the redactions. Redactions will be applied to documents being produced, and the production will therefore include any pertinent metadata.

7.5 Should a receiving party be unable to ascertain whether or not a redaction on the log is appropriate, the parties shall meet and confer to attempt to cooperatively resolve the dispute.

7.6 Privilege logs and redaction logs shall be produced within a reasonable time following production of the first production volume and shall be supplemented within a reasonable time following each subsequent production where production occurs on a rolling basis, or by another date upon agreement of the requesting and

producing parties. The parties, as appropriate, shall meet and confer to reach agreement regarding what constitutes such reasonable time.

8. MODIFICATION

8.1 This Order may be modified by agreement of the parties or by the Court for good cause shown.

SO ORDERED.

Date: September 9, 2020

/s/ Mitchell S. Goldberg

UNITED STATES DISTRICT JUDGE